

**REMARKS**

Claims 1-19 are currently pending in the subject application, and are presently under consideration. Claims 1-19 are rejected. Claims 1, 8 and 15 have been amended. Claims 10 and 13 have been cancelled. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

**I. Rejection of Claims 1-19 Under 35 U.S.C. §102**

Claims 1-19 stand rejected under 35 U.S.C. §102 as being anticipated by Wood, et al. (U.S. 6,668,322). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1 has been amended to recite generating a private/public key pair and transmitting the public key to a Public Key Infrastructure (PKI) system from a client platform. Wood discloses that a login credentials structure is encrypted using an authentication service's (of authentication component 130) public key (See Wood, Col. 7, Lines 16-18). The "authentication service's public key" disclosed in Wood does not correspond the public key recited in claim 1. The authentication service's public key is not generated and transmitted to a PKI system from a client platform as recited in claim 1, but is simply used to encrypt login credentials. Furthermore, claim 1 recites transmitting the public key to a domain certificate authority for signature. Wood discloses the use of the authentication service's public key for encrypting the login credential structure. Wood is silent on a domain certificate signing a public key generated from a client platform. Still further, claim 1 recites returning the public key to the client platform signed by the domain certificate authority to be used as a single sign-on role certificate. Wood discloses supplying a session token using a set cookie directive encoded with authentication results (See Wood, Col. 15, Lines 9-14). The "cookie directive" disclosed in Wood does not correspond to the signed public key recited in claim 1, because the signed public key recited in claim 1 is generated at a client platform. Accordingly, Wood does not disclose each and every element recited in claim 1. Therefore, Wood does not anticipate claim 1.

Claims 2-7 depend directly or indirectly from claim 1 and are not anticipated for the same reasons as claim 1 and for the specific elements recited therein. Therefore, claims 2-7 are not anticipated by Wood.

Claim 3 recites delivering a password to a user through the mail to the user's home address. Wood does not disclose delivering a password to a user through the mail. In fact, Wood is silent on any specific method of delivery of a password to a user. Accordingly, Wood does not disclose each and every element recited in claim 3. Therefore, Wood does not anticipate claim 3.

Claim 6 recites storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card, or other storage device. As stated above with respect to claim 1, Wood does not disclose returning a public key to a client platform signed by a domain certificate authority. Thus, Wood does not disclose storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card or other storage device as recited in claim 6. Therefore, claim 6 is not anticipated by Wood.

Claim 7 recites accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority. Wood is silent on accessing a foreign computer network using a signed public key, as recited in claim 7. Accordingly, claim 7 is not anticipated by Wood.

Amended claim 8 recites signaling a client platform to create a private/public key pair, and receiving the public key of the private/public key pair from a client platform. Wood discloses a login credentials structure is encrypted using the public key of an authentication service (See Wood, Col. 7, Lines 15-18). Wood does not disclose receiving a public key from a client platform. Furthermore, amended claim 8 recites transmitting the public key to a domain certificate authority for signature. Wood discloses the use of the authentication service's public key for encrypting login credentials. Still further, claim 8 recites returning the public key to the client signed by the domain certificate authority wherein the signed public is operative as a single sign-on role certificate. Wood discloses supplying a session token using a set cookie

directive encoded with authentication results (See Wood, Col. 15, Lines 9-14). The “cookie directive” disclosed in Wood does not correspond to the signed public key recited in claim 8. Accordingly, Wood does not disclose each and every element recited in claim 8. Therefore, Wood does not anticipate claim 8.

Claims 10 and 13 have been canceled such that their rejection is now moot.

Claims 9, 11-12 and 14 depend directly or indirectly from claim 8 and are not anticipated for the same reasons as claim 8 and for the specific elements recited therein. Therefore, claims 9, 11-12 and 14 are not anticipated by Wood.

Claim 14 recites accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority. Wood is silent on accessing a foreign computer network using a signed public key as recited in claim 14. Accordingly, claim 14 is not anticipated by Wood.

Amended claim 15 recites delivering a password to a user through the mail to the user's home address. Wood does not disclose sending a user a password through the mail. In fact, Wood is silent on any specific method of delivering a password to a user. Furthermore, claim 15 has been amended to recite generating a private/public key pair at a client platform and transmitting the public key of the private/public key pair to the PKI system from the client platform. Wood discloses a login credentials structure is encrypted using the public key of an authentication service (See Wood, Col. 7, Lines 15-18). Wood does not disclose generating a private/public key pair from a client platform, as recited in claim 15. Still further, amended claim 15 recites transmitting the public key to a domain certificate authority for signature. Wood is silent on a domain certificate signing a public key generated by a client platform. Furthermore, amended claim 15 recites returning the public key to the client platform signed by the domain certificate authority, wherein the signed public key is operative as a single sign-on role certificate. Wood discloses supplying a session token using a set cookie directive encoded with authentication results (See Wood, Col. 15, Lines 9-14). The “cookie directive” disclosed in Wood does not correspond to the signed public key recited in claim 15. Accordingly, Wood

does not disclose each and every element recited in claim 15. Therefore, Wood does not anticipate claim 15.

Claims 16-19 depend directly or indirectly from claim 15 and define over the prior art for the same reasons as claim 15 and for the specific elements recited therein. As discussed above claims 16-19 are not anticipated by Wood.

Claim 18 recites storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card, or other storage device. As stated above with respect to claim 15, Wood does not disclose returning a public key to a client platform signed by a domain certificate authority. Thus, Wood does not disclose storing the public key signed by the domain certificate authority in a hardware token, smart card, a computer, a magnetic strip card or other storage device as recited in claim 18. Therefore, claim 18 is not anticipated by Wood.

Claim 19 accessing a foreign computer network not associated with the PKI system using the public key signed by the domain certificate authority. Wood is silent on accessing a foreign computer network. Thus, Wood does not disclose using a signed public key to access a foreign network as recited in claim 19. Therefore, claim 19 is not anticipated by Wood.

For the reasons described above, claims 1-19 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

Serial No. 09/822,958

Docket No. NG(MS)7186NP

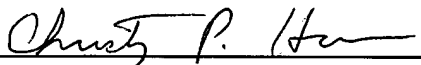
**CONCLUSION**

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 11 / 9 / 04

  
\_\_\_\_\_  
Christopher P. Harris  
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.  
526 SUPERIOR AVENUE, SUITE 1111  
CLEVELAND, OHIO 44114-1400  
Phone: (216) 621-2234  
Fax: (216) 621-4072